CLAIMS

What is claimed is:

1. A method for securely creating an endorsement certificate for a device in an insecure environment, said method comprising:

generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

creating a non-public, signing key pair that is injected into a plurality of valid devices;

verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and

inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device.

2. The method of Claim 1, further comprising:

providing a signing key certificate for said signing key pair, said signing key certificate including a public singing key of said signing key pair; and

forwarding said signing key certificate via a secure communication medium to said credential server.

3. The method of Claim 1, further comprising:

signing said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK); and

forwarding a resulting signed EK to said credential server to initiate a credential process.

4. The method of Claim 3, further comprising:

receiving said signed EK at said credential server;

comparing the public signing key within the signing key certificate with a signature from the signed EK; and

when the public signing key matches the signature, confirming said EK as originating from a valid device.

5. The method of Claim 1, wherein following said verifying step said method further comprises:

initially storing the credential in a database of said credential server;

monitoring for a request from a customer to provide said certificate to said device; and

following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

6. The method of Claim 1, wherein said endorsement certificate is once-writeable public-readable and is utilized for signing said public key during communication from and to said device.

7. The method of Claim 1, wherein said signing key pair is a single-use parameter, said method further comprising immediately destroying said signing key pair within said device following a creation of said EK.

8. The method of Claim 1, wherein said credential server is remotely located from a vendor manufacturing said device and said method comprises transmitting said signing key pair from said device to said credential server via a secure communication medium.

9. The method of Claim 1, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined method for determining when to switch from use of said first signing key pair to said second signing key pair, said pre-defined method selected from among:

expiration of a preset amount of device manufacturing time; and

manufacture of a preset number of devices during manufacture of the plurality of valid devices.

10. The method of Claim 1, wherein said device is a trusted platform module (TPM).

11. A TPM device manufactured and authenticated according to the steps of Claim 1.

12. A data processing system comprising:

a processor;

a trusted platform module (TPM) chip;

a bus for interconnecting said processor and said TPM chip;

a network interface with communication means for connecting said TPM to a secure credential server; and

means whereby said TPM is able to verify an endorsement key pair of said TPM as being a valid pair generated during manufacture of said TPM by utilizing a signing key pair injected by a TPM vendor into the TPM during manufacture of the TPM.

13. The data processing system of Claim 12, wherein said signing key pair has an associated signing key certificate that is sent to the secure credential server during manufacture of the TPM and said means for verifying an endorsement key pair further comprises:

means for signing a public value of said endorsement key pair with a public signing key of said signing key pair to generate a signed EK; and

means for forwarding said signed EK to said credential server, wherein said credential server returns an endorsement certificate only when the signed EK was generated within the TPM as confirmed by a comparison of the signed EK's public signing key with a public signing key of the signing key certificate.

14. A data processing system utilized for issuing endorsement certificates, comprising:

a processor;

a memory couple to said processor via an interconnect;

a security mechanism for ensuring optimum security of processes within said data processing system;

input/output mechanism for receiving a signing key certificate from a TPM vendor for utilization during a credential process for a specific group of manufactured TPM devices; and

secure communication means for receiving an endorsement key (EK) requesting issuance of an endorsement certificate, wherein said EK comprises a public endorsement key signed by a public signing key; and

program means for determining, by utilizing said public signing key and said signing key certificate, when said EK is an EK of an endorsement key pair that was generated within one of said manufactured TPM devices.

15. The data processing system of Claim 14, further comprising means for generating a certificate only when said public signing key matches a public signing key within said signing key certificate.

16. The data processing system of Claim 14, further comprising:

recording when a request for an EK certificate fails; and

tracking each failed request to identify TPM vendors with greater than a pre-established number of failures; and

messaging said TPM vendors to update their security procedures.

17. A system for securely creating an endorsement certificate for a TPM device in an insecure environment, said system comprising:

means for generating for a valid device an endorsement key pair that includes a private key and a public key, wherein said private key is not public readable;

means for creating a non-public, secure value that is provided to both a plurality of valid devices and a credential server;

means for verifying at a credential server that an endorsement key of a requesting device is a valid endorsement key generated during manufacture of said valid device by confirming a signature of said endorsement key is a public signing key of said signing key pair, wherein said credential server includes secure identification data of said non-public, signing key pair; and

means for inserting an endorsement certificate into said device to indicate that said device is an approved device by an OEM (original equipment manufacturer) of the device only when said endorsement key is confirmed having been generated from within a valid device.

18. The system of Claim 17, further comprising:

means for providing a signing key certificate for said signing key pair, said signing key certificate including a public singing key of said signing key pair; and

means for forwarding said signing key certificate via a secure communication medium to said credential server.

19. The system of Claim 18, further comprising:

means for combining said public key of the endorsement key pair with a public signing key of said signing key pair when creating the endorsement key (EK); and

means for forwarding a resulting signed EK to said credential server to initiate a credential process.

20. The system of Claim 19, further comprising:

means for receiving said EK at said credential server;

means for comparing the copy of the public signing key within the signing key certificate with a signature from the signed EK; and

means, when the public signing keys match, for confirming said EK as originating from a valid device.

21. The system of Claim 17, wherein following said verifying said system further comprises:

means for initially storing the credential in a database of said credential server;

means for monitoring for a request from a customer to provide said certificate to said device; and

means for following a receipt of said customer request, transmitting said certificate to said device to be inserted within the device.

22. The system of Claim 17, wherein said endorsement certificate is once-writeable and public-readable and is utilized for signing said public key during communication from and to said device.

23. The system of Claim 17, wherein said signing key pair is a single-use parameter, said system further comprising means for immediately destroying said value within said device following a creation of said EK.

24. The system of Claim 17, wherein said credential server is remotely located from a vendor manufacturing said device and said system comprises means for transmitting said signing key certificate from said device to said credential server via a secure communication medium.

25. The system of Claim 17, wherein the signing key pair is a first signing key pair that is provided to a first set of said plurality of valid devices and a second set of said plurality of valid devices are provided a second signing key pair, based on a pre-defined system for determining when to switch from utilizing said first signing key pair to utilizing said second signing key pair, said pre-defined system selected from among:

expiration of a preset amount of device manufacturing time; and

manufacture of a preset number of devices from the plurality of valid devices.